



**ANEXO 7:
REGLAMENTO ESPECÍFICO DE ACREDITACIÓN
PRESTADOR DE SERVICIOS DE VALOR AÑADIDO
(SVA)**

CAPÍTULO I DISPOSICIONES GENERALES

Artículo 1°.- Objeto

El presente Reglamento establece los criterios de acreditación de los Prestadores de Servicios de Valor Añadido (SVA), tanto públicos como privados; así como los derechos y obligaciones que deben de cumplir para poder ser acreditados por la Comisión de Reglamentos Técnicos y Comerciales (CRT) del INDECOPI, en su condición de Autoridad Administrativa Competente (AAC) conforme a ley.

Asimismo en todos los casos en que se haga mención al Reglamento, se entenderá referido al presente instrumento legal. En caso en que se haga mención al Reglamento General, se entenderá referido al Reglamento General de Acreditación de Prestadores de Servicios de Certificación Digital.

CAPÍTULO II DEFINICIONES

Artículo 2°.- Definiciones

Para efectos del presente Reglamento se aplican las definiciones establecidas contenidas en el Reglamento General de Acreditación de Prestadores de Servicios de Certificación Digital.

CAPÍTULO III ASPECTOS GENERALES DEL PROCEDIMIENTO DE ACREDITACIÓN COMO SVA

Artículo 3°.- Norma aplicable

El procedimiento de acreditación se rige en particular por lo establecido en el presente Reglamento en concordancia con la normativa contenida en el Reglamento General de Acreditación de Prestadores de Servicios de Certificación Digital.

En caso de conflicto entre estas dos normas, primará lo establecido en el presente Reglamento.

Artículo 4°.- Tipo de acreditación que se solicita

En el formato de solicitud que se presentará para efectos de la correspondiente acreditación, deberá especificarse el tipo de acreditación que se solicita, la misma que puede ser:

- a. Acreditación como SVA que realiza procedimientos sin firma digital de usuarios finales
- b. Acreditación como SVA que realiza procedimientos con firma digital de usuarios finales
- c. Renovación de la acreditación
- d. Acreditación por homologación

Artículo 5°.- Acreditación como SVA que realiza procedimientos sin firma digital de usuarios finales

La acreditación como SVA que realiza procedimientos sin firma digital de usuarios finales se solicita para los casos de servicios de valor añadido como Time Stamping, que no requieren en ninguna etapa de la prestación del servicio la firma digital del usuario final en documento o formulario alguno.

Artículo 6°.- Acreditación como SVA que realiza procedimientos con firma digital de usuarios finales

La acreditación como SVA que realiza procedimientos con firma digital de usuarios finales se solicita para los casos de servicios de valor añadido como el Sistema de Intermediación Electrónico, en donde se requiere en determinada etapa del procedimiento la firma digital por parte del usuario final en algún tipo de documento o formulario.

Para la acreditación como SVA que realiza procedimientos con firma digital de usuarios finales, se requiere el empleo de un aplicativo (software) que se encuentre acreditado conforme a lo establecido en el Reglamento para la acreditación de una aplicación (SW) de clave pública (PKI).

Artículo 7°.- Del almacenamiento digital o conservación de mensajes de datos

En el caso que como parte del servicio de valor añadido se opte por la conservación de algún tipo de mensaje de datos o documento electrónico, se deberá observar los requisitos y condiciones de validez establecidas para tales efectos por el Decreto Legislativo No. 681, mediante el cual se establecen las normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuanto a la producida por procedimientos informáticos en computadoras, así como sus normas complementarias y reglamentarias. Siendo necesario para tales efectos someterse al correspondiente procedimiento de acreditación de la línea de producción de las microformas, a fin que éstas puedan cumplir con el amparo legal a que se refiere la normativa de la materia.

La obtención de la acreditación para operar como SVA en cualquiera de sus modalidades no exime de la obligación de solicitar la acreditación a que se refiere el párrafo anterior, siempre que la entidad brinde adicionalmente el servicio de conservación o almacenamiento digital.

Artículo 8°.- Niveles de seguridad

En la solicitud de acreditación como SVA se deberá establecer el nivel de seguridad al que se postula, debiéndose para tales efectos cumplir con los lineamientos y requisitos exigidos en la Guía de Acreditación de Prestadores de Servicios de Valor Añadido – SVA y las condiciones técnicas particulares para el nivel de seguridad establecido.

Artículo 9°.- Nivel de seguridad medio

Los certificados de nivel de seguridad medio (M) están concebidos para:

- a. Trámites con el Estado en las transacciones económicas de monto bajo o medio y para el intercambio de documentos de riesgo bajo o medio.
- b. Información crítica y de seguridad nacional en redes cifradas.
- c. Acceso a información clasificada o información de acceso especial en redes protegidas.
- d. Aplicaciones de valor financiero medio o de comercio electrónico, tales como las planillas, contratos, compra de vehículos, etc.

Adicionalmente, este nivel de seguridad se aplica a los Prestadores de Servicios de Certificación Digital – PSC sin certificación; que sólo cuentan con la aprobación de las auditorías correspondientes para la acreditación o implementación de las normas correspondientes.

Artículo 10°.- Condiciones técnicas nivel de seguridad medio

Para efectos de las especificaciones técnicas se tendrán en consideración las siguientes precisiones:

- a. Los dispositivos criptográficos físicos –hardware y firmware (sistema operativo)– que almacenan las claves privadas de la entidad final –usuarios– deben de cumplir con la certificación FIPS 140-2 Nivel de Seguridad 1 (mínimo) o Common Criteria EAL4.
- b. La longitud de clave privada mínima debe ser de 1024 bits y el certificado debe ser renovado como máximo anualmente.
- c. Los certificados a nivel de entidad final –usuarios– deben ser generados de manera individual y separados para las siguientes funciones: cifrado y firma (no repudio) o autenticación. Las funciones de firma y autenticación son compatibles y pueden ser realizadas con un mismo certificado.

Artículo 11°.- Nivel de seguridad medio alto

Los certificados de Nivel de Seguridad Medio Alto (M+) están concebidos para:

- a. Todas las aplicaciones apropiadas para certificados de Nivel de Seguridad Medio (M).
- b. Intercambio de documentos y transacciones monetarias de alto riesgo, y trámites con el Estado en las transacciones económicas de alto monto y alto riesgo.
- c. Información crítica no clasificada o de seguridad nacional en una red no cifrada.
- d. Acceso a información clasificada o información de acceso especial en redes no protegidas.
- e. Aplicaciones de valor financiero de riesgo y monto medio alto o de comercio electrónico.

Adicionalmente, este nivel de seguridad se aplica a los Prestadores de Servicios de Certificación Digital – PSC con las siguientes certificaciones:

- ER: ISO 9001:2000
- EC: ISO 27001
- SVA: ISO 9001:2000 o ISO 27001, y SW con ISO 9001:2000 o CMMI nivel 2 (mínimo)

Artículo 12°.- Condiciones técnicas del nivel de seguridad medio alto

Para efectos de las especificaciones técnicas se tendrán en consideración las siguientes precisiones:

- a. Los dispositivos criptográficos físicos –hardware y firmware (sistema operativo)– que almacenan las claves privadas de la entidad final –usuarios– deben de cumplir con la certificación FIPS 140-2 Nivel de Seguridad 2 (mínimo) o Common Criteria EAL4+.
- b. La longitud de clave privada mínima debe ser de 2048 bits y el certificado debe ser renovado como máximo cada dos (2) años.
- c. Los certificados a nivel de entidad final –usuarios– deben ser generados de manera individual y separados para las siguientes funciones: cifrado, firma (no repudio) y autenticación.

Artículo 13°.- Renovación de acreditación

La renovación de acreditación se rige por lo establecido en el Capítulo VII del presente Reglamento.

Artículo 14°.- Acreditación por homologación

La acreditación por homologación se rige por el procedimiento establecido en el Capítulo VII del presente Reglamento.

CAPÍTULO IV SOLICITUD DE ACREDITACIÓN Y DOCUMENTOS SUSTENTATORIOS

Artículo 15°.- Solicitud de acreditación como SVA

La solicitud de acreditación será dirigida al Secretario Técnico de la Comisión de Reglamentos Técnicos y Comerciales del INDECOPI, especificando el tipo de acreditación que se solicita y el nivel de seguridad al que se postula.

La solicitud será realizada en base a la Ficha de Solicitud de Acreditación como Prestador de Servicios de Valor Añadido (SVA).

Artículo 16°.- Los documentos que se deben acompañar a la mencionada Ficha de Solicitud de Acreditación, son los que se detallan a continuación:

- a. Copia simple del documento de identidad del solicitante.
- b. Documentos que acrediten la existencia y vigencia de la persona jurídica solicitante.
- c. Documentos que acrediten los poderes en virtud a los cuales los representantes legales se encuentran facultados para solicitar la acreditación.
- d. Memoria descriptiva y organigrama estructural o funcional.

- e. Documentos que acrediten domicilio en el país.
- f. Declaración jurada de contar con infraestructura e instalaciones necesarias, según el nivel de seguridad solicitado.
- g. Declaración jurada de aceptación de las auditorías, cuando la AAC lo requiera.
- h. Declaración de Prácticas de Valor Añadido (VAPS).
- i. Declaración jurada declarando cumplir con tener operativo software, hardware y demás componentes adecuados para las prácticas de valor añadido y las condiciones de seguridad adicionales basadas en estándares internacionales o compatibles a los internacionalmente vigentes que aseguren interoperabilidad.
- j. Constancia de pago de los derechos administrativos
- k. Documento donde conste el mapeo correspondiente: VAPS vs. Marco de la Política de Prestación de Servicios de Valor Añadido (anexo 1 de Guía de Acreditación de Prestadores de Servicios de Valor Añadido – SVA). Será requerido para el caso de los Sistemas de Intermediación Electrónico (SIE) que no hubieran elaborado su VAPS de acuerdo al esquema establecido en el mencionado documento.
- l. Contrato con la Entidad de Certificación emisora de los certificados digitales de autenticación empleados dentro del sistema del servicio brindado. Será requerido para el caso de los Sistemas de Intermediación Electrónicos (SIE) que ofrezcan el servicio de domicilio electrónicos.

Los documentos que se acompañen deberán encontrarse en idioma español. Si las fuentes originales provinieran de otro idioma, éstas deberán ser traducidas de manera oficial.

La relación de documentos antes señalada no es taxativa. En tal sentido, la CRT podrá considerar y solicitar cualquier documentación adicional que sea necesaria a efectos de poder tomar una decisión informada sobre la acreditación o no del solicitante.

Los documentos deberán estar conforme a lo establecido en la Guía de Acreditación de Prestadores de Servicios de Valor Añadido – SVA versión 3.3 y sus anexos, según corresponda.

Artículo 17°.- Acreditación de la existencia y vigencia de la persona jurídica

La existencia y vigencia de la persona jurídica deberá acreditarse con el documento de vigencia respectivo expedido por los Registros Públicos o mediante la especificación de la norma legal de creación de la persona jurídica correspondiente.

En el caso de empresas constituidas en el extranjero, se acreditará su existencia y vigencia mediante un certificado de vigencia de la sociedad u otro instrumento equivalente expedido por autoridad competente en su país de origen.

En el caso de las instituciones del Estado, deberán acreditar la existencia de una Oficina, Gerencia o dependencia interna a la cual se le otorgan funciones como prestador de servicios de valor añadido.

Artículo 18°.- Acreditación de los poderes de los representantes legales

Para la verificación de las facultades de los representantes legales, se tendrán en cuenta las reglas siguientes:

- a. En el caso de personas jurídicas constituidas en el país: en el documento que acredite la representación, deberán constar las facultades conferidas al representante, bastando para tales efectos la presentación de la copia del poder respectivo.
- b. En el caso de personas jurídicas constituidas en el extranjero: los correspondientes poderes deberán ser legalizados por un funcionario consular peruano y de encontrarse redactados en idioma extranjero, será necesario que sean traducidos, debiendo el responsable de la traducción suscribir el correspondiente documento.
- c. En el caso de instituciones del Estado, deberá acreditarse el nombramiento de la persona encargada de dirigir la oficina, gerencia o dependencia interna encargada de la prestación de servicios de valor añadido. Debiéndose asimismo acreditarse las facultades de este funcionario.

Artículo 19°.- Memoria descriptiva – Organigrama Estructural y Funcional

La memoria descriptiva y el organigrama estructural y funcional deberán ser realizados conforme al Formato denominado: Memoria Descriptiva y Organigrama Estructural y Funcional – Prestador de Servicios de Valor Añadido (SVA).

Artículo 20°.- Documentos que acrediten domicilio en el país

La condición de domiciliada de un SVA solicitante, se acredita con el comprobante de inscripción de la persona jurídica en el Registro Único de Contribuyentes (R.U.C.), donde debe constar con la condición de “habida”.

En su defecto, se podrá acompañar cualquier otra documentación que sirva para acreditar la condición de domiciliado en el país, la misma que será materia de evaluación por parte de la Comisión de Reglamentos Técnicos y Comerciales.

Artículo 21°.- Declaración de Prácticas de Valor Añadido (VAPS)

La Declaración de Prácticas Valor Añadido es el documento en el que constan de manera detallada las políticas y procedimientos que aplica el Prestador de Servicios de Valor Añadido para la prestación de sus servicios.

Este documento deberán cumplir con las especificaciones a que se refieren los dos siguientes artículos del presente reglamento.

Artículo 22°.- Declaración de Prácticas de Prestación de Servicios de Valor Añadido de SVA para Autoridades de Sellado de Tiempo (*Time Stamping Authority*)

La Declaración de Prácticas de Prestación de Servicios de Valor Añadido de SVAs que operen bajo esta modalidad, deberán observar los lineamientos establecidos por el RFC 3628: *Policy Requirements for Time-Stamping Authorities (TSAs)*, en concordancia con el estándar ISO/IEC 18014-1:2002 “*Information technology -- Security techniques -- Time-Stamping Services -- Parte 1: Framework*”.

Asimismo, se deberán cumplir con los principios de privacidad recogidos en la Norma Marco sobre Privacidad.

Artículo 23°.- Declaración de Prácticas de Prestación de Servicios de Valor Añadido de SVA para Sistemas de Intermediación Electrónicos

La Declaración de Prácticas de prestación de servicios de valor añadido de SVAs que operen bajo esta modalidad, deberán observar los lineamientos establecidos en el documento Marco de la Política de Prestación de Servicios de Valor Añadido.

Asimismo, se deberán cumplir con los principios de privacidad recogidos en la Norma Marco sobre Privacidad.

Artículo 24°.- Constancia de pago de los derechos administrativos

Los derechos administrativos que deben cancelarse para efectos del procedimiento de acreditación como SVA, asciende al 100% del valor de la UIT.

Artículo 25°.- Documentación para la realización de evaluación técnica

Para efectos de la documentación que se debe acompañar para efectos de la realización de la evaluación técnica, deberá tomarse en cuenta lo siguiente:

- a. La Declaración de Prácticas de Valor Añadido (VAPS) deberá estar elaborada en estricta observancia de los lineamientos establecidos en el documento Marco de la Política de Prestación de Servicios de Valor Añadido.
En el caso que la VAPS no se haya elaborado siguiendo la estructura del mencionado documento, deberá acompañarse uno donde conste un mapeo correspondiente entre la VAPS del solicitante y los lineamientos establecidos en el mencionado documento.

- b. En el caso de un SVA que realiza procedimientos con firma digital de usuarios finales, deberá acompañarse el documento en el que conste la acreditación por parte de la CRT del software empleado para el servicio de valor añadido que presta. En el caso que este software no sea un desarrollo propio del SVA solicitante, deberá acompañarse el documento en el que conste la autorización para su uso por parte del propietario del mismo.
- c. En el caso de un SVA en la modalidad de Sistema de Intermediación Electrónico, que como parte de su servicio ofrezca certificados digitales de autenticación –de uso exclusivo dentro del sistema del servicio brindado–, deberá presentarse el respectivo contrato con la Entidad de Certificación emisora. Dichos certificados digitales deberán cumplir como mínimo con los requerimientos del nivel de seguridad medio.

Artículo 26°.- Declaraciones juradas

Las declaraciones juradas a que se alude en los incisos f), g) y i) del artículo 16° forman parte integrante de la Ficha de Solicitud de Acreditación como Prestador de Servicios de Valor Añadido (SVA), por lo que bastará la suscripción de este documento para que se entiendan efectuadas las mencionadas Declaraciones Juradas.

Sin perjuicio de lo regulado en el párrafo anterior, el SVA solicitante podrá elaborar las mencionadas Declaraciones Juradas en documentos independientes, los mismos que deberán ser acompañados a la solicitud de acreditación.

CAPÍTULO V EVALUACIÓN DOCUMENTARIA Y TÉCNICA

Artículo 27°.- Evaluación documentaria

Dentro del procedimiento de acreditación, la etapa de evaluación documentaria será llevada a cabo en estricta observancia de lo establecido en el Reglamento General.

Artículo 28°.- Comité Evaluador

En la resolución en la que se declara la procedencia de la solicitud de acreditación se designará al Comité Evaluador encargo de llevar a cabo la misma.

Entre los miembros del Comité Evaluador y el solicitante no deberá existir ningún tipo de vinculación directa o indirecta que pueda comprometer la imparcialidad.

En caso que el SVA no se encuentre conforme con la designación de alguno de los miembros del comité evaluador, podrá efectuar las correspondientes observaciones, debiendo observar las condiciones y requisitos establecidos para estos efectos por el Reglamento General.

Artículo 29°.- Evaluación técnica

Dentro del procedimiento de acreditación como SVA, la evaluación técnica se divide en dos etapas:

- a. Evaluación de la VAPS, la Política y el Plan de Privacidad, la Política de Seguridad y los requerimientos de Usabilidad
- b. Evaluación de interoperabilidad

El procedimiento de evaluación técnica se rige por los lineamientos establecidos para tales efectos por el Reglamento General.

En ambas etapas, el Comité evaluador deberá emitir pronunciamiento claro y debidamente fundamentado.

Artículo 30°.- Evaluación de la VAPS, la Política y el Plan de Privacidad, la Política de Seguridad y los requerimientos de Usabilidad

El objetivo de esta evaluación es examinar la adecuación de la VAPS, la Política y el Plan de Privacidad, la Política de Seguridad y los requerimientos de Usabilidad del SVA solicitante con el documento Marco de la Política de Prestación de Servicios de Valor Añadido, la Norma Marco sobre Privacidad y el Modelo de Política de Seguridad, respectivamente.

El procedimiento para la evolución se realizará sobre la base de los documentos acompañados para tales efectos por el SVA solicitante.

De considerarlo necesario, el Comité Evaluador podrá solicitar documentación complementaria o la realización de una evaluación o auditoría en las instalaciones del SVA.

Artículo 31°.- Evaluación de interoperabilidad

El objetivo de la evaluación de interoperabilidad es establecer el cumplimiento de las condiciones necesarias para el establecimiento de interoperabilidad entre el SVA solicitante mediante el uso de la TSL –ETSI TS102.231–, como estándar para la creación de la lista segura de proveedores de servicios de certificación digital.

Para el procedimiento de evaluación de interoperabilidad, se tomará contacto con el personal designado para tales efectos por el SVA solicitante, a fin de realizar las pruebas correspondientes.

Artículo 32°.- TSL de prueba

La TSL de prueba que se genere durante la etapa de evaluación de interoperabilidad deberá ser alojada en la infraestructura tecnológica del SVA solicitante a efectos de realizar las pruebas correspondientes,

Esta TSL únicamente tiene carácter de prueba y por ende no podrá ser utilizado por el SVA solicitante para otros fines.

CAPITULO VI DE LA ACREDITACIÓN COMO SVA

Artículo 33°.- Alcances de la acreditación


La acreditación como SVA implica el ingreso del solicitante a la IOFE y su inscripción en el Registro de PSC acreditados, permitiéndole asimismo gozar de los beneficios, presunciones y efectos legalmente establecidos. Asimismo, una vez acreditado, el SVA solicitante ingresará a la TSL que para tales efectos mantiene la CRT en su condición de AAC.

El procedimiento formal de acreditación como SVA se rige por lo establecido en el Reglamento General.

Artículo 34°.- Efectos de la acreditación

Una vez obtenida la correspondiente acreditación, el SVA se encuentra obligado a prestar sus servicios en los mismos términos a los contenidos en la VAPS que fueran materia de evaluación por parte de la AAC.

Asimismo, deberá cumplir en todo momento las obligaciones a que se refiere el Reglamento de la Ley de Firmas y Certificados Digitales.

	Infraestructura Oficial de Firma Electrónica IOFE PERU	Rev: 03/23-02-2007
		Aprobado:

**CAPITULO VII
DEL MANTENIMIENTO, RENOVACIÓN Y HOMOLOGACIÓN DE LA ACREDITACIÓN**

Artículo 35°.- Aplicación supletoria del Reglamento General

El mantenimiento, renovación y homologación de la acreditación se rige por lo establecido en el Reglamento General de Acreditación de Prestadores de Servicios de Certificación Digital.